UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/773,394	02/06/2004	Shehzad T. Merchant	02453.0020.NPUS00	6341

27194 7590 11/27/2007

HOWREY LLP
C/O IP DOCKETING DEPARTMENT
2941 FAIRVIEW PARK DRIVE, SUITE 200
FALLS CHURCH, VA 22042-2924

EXAMINER	
NGUYEN, MINH DIEU T	
ART UNIT	**PAPER NUMBER**
2137	

MAIL DATE	DELIVERY MODE
11/27/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/773,394	MERCHANT ET AL.	
	Examiner	Art Unit	
	Minh Dieu Nguyen	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 September 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) *29-38* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to amendments

1. This office action is in response to the communication dated 9/17/2007 with the election of claims 1-28.

2. Claims 1-28 are pending. Claims 29-38 are being withdrawn as being directed to a non-elected invention.

Response to arguments

3. Applicant's arguments dated 9/17/2007 have been considered but are moot in view of the new ground(s) of rejection.

Drawings

4. The objection of the drawings has been withdrawn based on the filed amendments.

Specification

5. The objection of the specification has been withdrawn based on the filed amendments.

Claim Objections

6. Claims 1-3 and 8-10 are objected to because of the following informalities:

a) As to claim 1, the phrase "the device becomes operational" should be -- the **network** device becomes operational-- and "the device inoperative at

least in part and removing the sensitive information from the device" should be -- the **network** device inoperative at least in part and removing the sensitive information from the **network** device--.

b) As to claims 2-3 and 9-10, the phrases "a group consisting of" should be --**the** group consisting of-- according to Markush claim format (MPEP 803.02)..

c) As to claim 8, the phrase "the device becomes operational" should be --the **network** device becomes operational--; the phrase "the device is disconnected from the network" should be –the **network** device is disconnected from the network-- and "thereby rendering the device inoperative" should be – thereby rendering the **network** device inoperative--.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-2, 4-9, 11-15, 19, 22 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Guy et al. (2005/0114473).

a) As to claim 8, Guy discloses a method for protecting sensitive information in a network, comprising: storing the sensitive information at a

network component; attaching a network device to the network, the network device lacking the sensitive information and being inoperative, at least in part, until the sensitive information is stored therein; downloading the sensitive information from the network component to the network device; storing the sensitive information in the network device so that the network device becomes operational on the network (i.e. the program code that is downloaded to access point 22 in the programming phase is held in a configuration file in a memory 56 of hub 26, at startup or reset of system 20, a central processing unit (CPU) 54 reads the configuration file from memory 56, and outputs the program code from the configuration file to interface 48 by writing successive words of the code to register 52, processor 50 converts the code words to an appropriate binary form for transmission over the LAN via PHY device 42, **Guy**: Fig. 2, 0059; when the access point starts up (typically at power-up or reset of the WLAN), program code is downloaded to the access point over the LAN, and is loaded directly via the LAN interface into the FPGA. Once the code is loaded, the FPGA is ready to perform its communication functions in the WLAN. Upon power-up or reset of access point 22, hub 26 downloads generic, start-up program code to processor 44. The purpose of this start-up code is to cause the processor to read the value of component 45, and to report the value back via LAN 28 to hub 26. Based on this value, CPU 54 determines the version of operational program code to be downloaded subsequently to this particular access point, **Guy**: 0004, 0075; the access points include substantially no non-volatile memory for storing the program code, **Guy**: 0040); when the network device is disconnected from

the network, erasing the sensitive information from the network device, thereby rendering the network device inoperative, at least in part (i.e. Automatic programming of processor 44 may occur not only when system 20 is initially switched on or reset, but also when a new access point 22 is connected to the system during operation. Some Ethernet PHY devices are capable of automatic link detection. In any case, when MAC processor 50 receives a link detection signal, it notifies CPU 54, which then downloads the appropriate program code to the new access point, **Guy**: 0077). As such, when the network device is not connected to the network (i.e. power lost or power is reset), the operational program code stored in no non-volatile memory is lost, hence the network device is not operational).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of disconnecting the network device (i.e. providing no power to the network device), erase the sensitive information from the network device, thereby rendering the network device inoperative in the system of Guy so as to securely control the program code.

b) As to claim 1, this claim is hardware implementation of the method of claim 8, and is rejected by a similar rationale applied against claim 8.

c) As to claims 2 and 9, Guy discloses the sensitive information is selected from the group consisting of configuration information, a software image, and a combination of the forgoing (**Guy**: 0059).

d) As to claims 4 and 11, Guy discloses the network device includes a volatile memory for storing the sensitive information (**Guy**: 0040).

e) As to claims 5 and 12, Guy discloses the network component is a LAN switch (**Guy**: 0076).

f) As to claims 6, 13, 19 and 25, Guy discloses the network device is a wireless access point (**Guy**: Fig. 1, element 22).

g) As to claims 7 and 14, Guy discloses the network component is located in a secure environment (**Guy**: 0008).

h) As to claims 15 and 22, the majority of limitations are addressed in claim 8 above.

9. Claims 3 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Guy et al. (2005/0114473) and further in view of Gerba et al. (2002/0040389).

Guy discloses the system of claim 2, however he is silent on the capability of having the configuration information is selected from the group consisting of a password, a user ID, a network security key, and any combination of the forgoing.

Gerba is relied on for the teaching of having the configuration information is selected from the group consisting of a password, a user ID, a network security key, and any combination of the forgoing (**Gerba**: 0072, 0074).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having the configuration information is selected from the group consisting of a password, a user ID, a network security key, and any combination of the forgoing in the system of Guy, as Gerba

teaches, so as to provide a wide variety of the type of data to select from for increasing versatility.

10. Claims 16-18 and 23-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Guy et al. (2005/0114473) and further in view of Loison et al. (2003/0046529).

Guy discloses the device of claim 15, however he is silent on the capability of the downloading means includes a bootstrap program for downloading from the network an executable image, wherein the executable image permits the device to download the configuration information and storing the executable image in the memory.

Loison is relied on for the teaching of the downloading means includes a bootstrap program for downloading from the network an executable image, wherein the executable image permits the device to download the configuration information and storing the executable image in the memory (i.eThe PXE protocol requires an appropriately configured BIOS and boot ROM which, when the computer is powered up, are effective to broadcast a general DISCOVER signal which is intended eventually to reach a local Intranet DHCP (Dynamic Host Configuration Protocol) server which, in turn, provides the client machine with a list of appropriate available boot servers. Using a low level protocol such as TFTP, the client machine then downloads the required boot image from an appropriate boot server and executes the boot image, **Loison**: 0006; upon receipt of an acceptable boot image 30, the image is transferred and/or copied to

a volatile (e.g. RAM) part of the computer's system memory 32 where the boot image is executed, in the following way. Execution of the boot image 30 in a boot image execution environment 33 effects a further download of required operating software images such as an appropriate Operating System, **Loison**: 0085).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of the downloading means includes a bootstrap program for downloading from the network an executable image, wherein the executable image permits the device to download the configuration information and storing the executable image in the memory in the system of Guy, as Loison teaches, so as to effectively provide a executable boot image.

11. Claims 20-21 and 26-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Guy et al. (2005/0114473) and further in view of Nessett et al. (6,766,453).

a) As to claims 20 and 26, Guy discloses the device of claim 19, however he is silent on the capability of the configuration information includes security information for allowing end user devices to access the network through the wireless access point.

Nesset is relied on for the teaching of the configuration information includes security information for allowing end user devices to access the network through the wireless access point (**Nessett**: col. 2, lines 47-54, Fig. 2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of the configuration information includes security information for allowing end user devices to access the network through the wireless access point in the system of Guy, as Nesset teaches, so as to securely accessing WLAN network (**Nessett**: col. 2, lines 34-37).

b) As to claims 21 and 27-28, Nesset discloses the configuration information includes security information for allowing the device access to the network and means for authenticating the device on the network (**Nessett**: col. 2, lines 54-57; col. 6, lines 14-32).

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-

direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MinhDieu Nguyen
11/26/07